REMARKS

This communication is responsive to the Office Action mailed December 4, 2007. The claims were previously rejected as being anticipated by Montville. After Applicant amended the claims to clarify that the service processes at least a portion of the request "using a private key associated with the service," the Examiner changed the rejection to be an obviousness rejection over Montville and further in view of Adams.

The claims have been further amended to clarify that communication between the "sender's side" and the "service" is via a network. The claims recite that the "service" determines a result using a private key associated with the service and, further, that the private key is kept secret by the service.

These features are supported by the specification at, for example, **[0017]** and **[0027]**, which read (emphasis added):

> **[0017]** For example, upon detecting an e-mail message to be sent, programming code either embedded within the email client or included as an add-on component intercepts the e-mail message. The mail client interacts with the service 104, in the form of a single TCP/IP request using a standard Internet protocol such as HTTP or HTTPS. By using standard Internet protocols communication with the service 104, packets of the communication will generally not be blocked by corporate or home DSL firewalls. Packets transmitted by HTTPS are also generally immune from network snooping since HTTPS is a secure protocol. It is noted that payload data of HTTP transmissions may be internally encrypted.

and

> **[0027]** Still at step 114, the service 104 signs the result (entire, or a portion thereof as discussed above) of the SHA-1 algorithm with a private key, such that it can be decoded using the corresponding public key. The private key is kept secret by the service 104, and the public key is made available to the receiver side 106. In some embodiments, the public key is "embedded" within the receiver side e-mail client software. The signing determines a sequence result that is an alphanumeric sequence of characters approximately 128 characters long. The service-determined sequence result is returned from the service 104 to the requesting sender 102. In some embodiments, a corresponding result code is also provided to the sender 102.

Adams is very clear that the mobile client includes the private key, and it is the mobile client that determines a "result" using a private key. Adams' mobile client is clearly not part of the service. For example, [0075] of Adams reads in part: "The messaging client 60 determines the messaging services with which the mobile device 38 has been configured to operate." Adams further reads, at [0075], "...the messaging client 60 determines for which messaging

services a private key has been loaded into a key store on the mobile device." Thus, with Adams, the private key is not kept secret by the service. In fact, with Applicant's claimed invention, the sender's side has no need for the private key associated with the service, since the service itself uses the private key to generate the "result," which is then provided back to the sender's side for incorporation into the e-mail message. (In fact, if the sender's side obtained the private key, it would breach the security and integrity of the service, since the service could then be spoofed using the thus-obtained private key. The private key is truly associated with and identified with the service and is not merely associated with a user of the service.)

Furthermore, the Examiner's stated rationale for modifying Montville in view of Adams is flawed. The Examiner states: "The suggestion/motivation for doing so would have been normally there are different private encryption keys and signature keys required for a service," referring to [0075] of Adams. However, what Adams states is that for each messaging service (which is not the same as the "service" recited in Applicant's claim in any event, in which the "service" is clearly distinct from the "e-mail system"), the messaging client must use a private encryption key for that service. However, according to the Examiner's interpretation of what is a "service," Montville only discloses using one "service" and, therefore, there is no need to incorporate the feature disclosed in Adams of loading a private encryption key for each of multiple services.

CONCLUSION

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER LLP

/ASH/
Alan S. Hodes
Reg. No. 38,185

P.O. Box 70250
Oakland, CA 94612-0250
408-255-8001